IN THE CLAIMS:

1. (Currently Amended) A cipher strength evaluation apparatus for evaluating strength on ciphertext outputted by a Feistel encryption apparatus having a plurality of steps of accepting unstirred text, stirring with an extended key, and calculating stirred text for encrypting plaintext step by step, the cipher strength evaluation apparatus comprising:

an estimated plaintext calculating part for accepting predetermined-step stirred text being stirred text at a predetermined step, calculating an estimated parameter A_s estimated as a parameter A_s determined from a predetermined-step extended key being an extended key at a predetermined step, and calculating estimated plaintext based on the predetermined-step stirred text and the estimated parameter A;

an encryption control part for using and allowing an encryption apparatus to calculate estimated ciphertext based on the estimated plaintext calculated by the estimated plaintext calculating part;

a key verification part for formulating an encryption equation with higher order differences based on the predetermined-step stirred text accepted by the estimated plaintext calculating part and the estimated ciphertext calculated under the control of the encryption control part, processing it by an algebraic technique to try to calculate a last-step estimated extended key estimated as an extended key at a last step, verifying the parameter A_s to be right by detecting that the last-step estimated extended key can be calculated, calculating a right last-step estimated extended key with a predetermined probability, and outputting a calculation impossible signal when detecting that calculation is impossible; and

a decryption control part for accepting the calculation impossible signal, and controlling the estimated plaintext calculating part, the encryption control part, and the key verification part to allow the last-step estimated extended key to be calculated.

2. (Currently Amended) A cipher strength evaluation apparatus for evaluating strength on ciphertext outputted by a Feistel encryption apparatus having a plurality of steps of accepting unstirred text, stirring with an extended key, and calculating stirred text for encrypting plaintext step by step, the cipher strength evaluation apparatus comprising:

an estimated plaintext calculating part for accepting predetermined-step stirred text being stirred text at a predetermined step, calculating an estimated parameter A_s estimated as a parameter A_s determined from a predetermined-step extended key being an extended key at a predetermined step, and calculating estimated plaintext based on the predetermined-step stirred text and the estimated parameter A;

an encryption control part for using and allowing an encryption apparatus to calculate estimated ciphertext based on the estimated plaintext calculated by the estimated plaintext calculating part;

a second predetermined-step estimated stirred text calculating part for accepting the estimated ciphertext calculated under the control of the encryption control part, calculating a last-step estimated extended key estimated as an extended key at the last step, and calculating second predetermined-step estimated stirred text estimated as stirred text at a second predetermined step based on the estimated ciphertext and the last-step estimated extended key;

a key verification part for formulating an encryption equation with higher order differences based on the predetermined-step stirred text accepted by the estimated plaintext

calculating part and the second predetermined-step estimated stirred text calculated by the second predetermined-step estimated stirred text calculating part, processing it by an algebraic technique to try to calculate a second predetermined-step estimated extended key estimated as an extended key at the second predetermined step, verifying the parameter A_1 and the last-step estimated extended key to be right by detecting that the second predetermined-step estimated extended key can be calculated, and outputting a calculation impossible signal when detecting that calculation is impossible; and

a decryption control part for accepting the calculation impossible signal, and controlling the estimated plaintext calculating part, the encryption control part, the second predetermined-step estimated stirred text calculating part, and the key verification part to allow the second predetermined-step estimated extended key to be calculated.

3. (Currently Amended) A cipher strength evaluation apparatus for evaluating strength on ciphertext outputted by a Feistel encryption apparatus having a plurality of steps of accepting unstirred text, stirring with an extended key, and calculating stirred text for encrypting plaintext step by step, the cipher strength evaluation apparatus comprising:

an estimated plaintext calculating part for accepting first-step stirred text being stirred text at a first step, calculating an estimated parameter A_1 estimated as a parameter A_1 determined from a first-step extended key being an extended key at the first step by exhaustive search, and calculating estimated plaintext based on the first-step stirred text and the estimated parameter A;

an encryption control part for using and allowing an encryption apparatus to calculate estimated ciphertext based on the estimated plaintext calculated by the estimated plaintext calculating part;

a key verification part for formulating an encryption equation with higher order differences based on the first-step stirred text accepted by the estimated plaintext calculating part and the estimated ciphertext calculated under the control of the encryption control part, processing it by an algebraic technique to try to calculate a last-step estimated extended key estimated as an extended key at a last step, verifying the parameter A_s to be right by detecting that the last-step estimated extended key can be calculated, calculating a right last-step estimated extended key with a predetermined probability, and outputting a calculation impossible signal when detecting that calculation is impossible; and

a decryption control part for accepting the calculation impossible signal, and controlling the estimated plaintext calculating part, the encryption control part, and the key verification part to allow the last-step estimated extended key to be calculated.

4. (Currently Amended) A cipher strength evaluation apparatus for evaluating strength on ciphertext outputted by a Feistel encryption apparatus having a plurality of steps of accepting unstirred text, stirring with an extended key, and calculating stirred text for encrypting plaintext step by step, the cipher strength evaluation apparatus comprising:

an estimated plaintext calculating part for accepting first-step stirred text being stirred text at a first step, calculating an estimated parameter A_s estimated as a parameter A_s determined from a first-step extended key being an extended key at the first step by exhaustive

search, and calculating estimated plaintext based on the first-step stirred text and the estimated parameter A;

an encryption control part for using and allowing an encryption apparatus to calculate estimated ciphertext based on the estimated plaintext calculated by the estimated plaintext calculating part;

[[an]] a predetermined-step estimated stirred text calculating part for accepting the estimated ciphertext calculated under the control of the encryption control part, calculating a last-step estimated extended key estimated as an extended key at the last step, and calculating predetermined-step estimated stirred text estimated as stirred text at a predetermined step based on the estimated ciphertext and the last-step estimated extended key;

a key verification part for formulating an encryption equation with higher order differences based on the first-step stirred text accepted by the estimated plaintext calculating part and the predetermined-step estimated stirred text calculated by the predetermined-step estimated stirred text calculating part, processing it by an algebraic technique to try to calculate a predetermined-step estimated extended key estimated as an extended key at the predetermined step, verifying the parameter A and the last-step estimated extended key to be right by detecting that calculation is possible, and outputting a calculation impossible signal when detecting that calculation is impossible; and

a decryption control part for accepting the calculation impossible signal, and controlling the estimated plaintext calculating part, the encryption control part, the predetermined-step estimated stirred text calculating part, and the key verification part to allow the predetermined-step estimated extended key to be calculated.

5. (Currently Amended) A cipher strength evaluation apparatus for evaluating strength on ciphertext outputted by a Feistel encryption apparatus having a plurality of steps of accepting unstirred text, stirring with an extended key, and calculating stirred text for encrypting plaintext step by step, the cipher strength evaluation apparatus comprising:

an estimated plaintext calculating part for accepting first-step stirred text being stirred text at a first step, calculating an estimated parameter A_1 estimated as a parameter A_1 determined from a first-step extended key being an extended key at a first step by exhaustive search, and calculating estimated plaintext based on the first-step stirred text and the estimated parameter A;

an encryption control part for using and allowing an encryption apparatus to calculate estimated ciphertext based on the estimated plaintext calculated by the estimated plaintext calculating part;

a last-but-one-step estimated stirred text calculating part for accepting the estimated ciphertext calculated under the control of the encryption control part, calculating a last-step estimated extended key estimated as an extended key at a last step by exhaustive search, and calculating last-but-one-step estimated stirred text estimated as stirred text at a last-but-one step being a preceding step of the last step based on the estimated ciphertext and the last-step estimated extended key;

a key verification part for formulating an encryption equation with higher order differences based on the first-step stirred text accepted by the estimated plaintext calculating part and the last-but-one-step estimated stirred text calculated by the last-but-one-step estimated stirred text calculating part, processing it by an algebraic technique to try to calculate a last-but-

one-step extended key estimated as an extended key at the last-but-one step, verifying the parameter A_1 and the last-step estimated extended key to be right by detecting that calculation is possible, and outputting a calculation impossible signal when detecting that calculation is impossible; and

a decryption control part for accepting the calculation impossible signal, and controlling the estimated plaintext calculating part, the encryption control part, the last-but-one-step estimated stirred text calculating part, and the key verification part to allow the last-but-one-step extended key to be calculated.

6. (Currently Amended) A cipher strength evaluation apparatus for evaluating strength on ciphertext outputted by a Feistel encryption apparatus having a plurality of steps of accepting unstirred text, stirring with an extended key, and calculating stirred text for encrypting plaintext step by step, the cipher strength evaluation apparatus comprising:

an estimated stirred text calculating part for accepting the plaintext satisfying a predetermined condition, calculating an estimated parameter A_1 estimated as a parameter A_1 determined from a first-step extended key being an extended key at a first step, and calculating predetermined-step estimated stirred text satisfying a predetermined condition and estimated as stirred text at a predetermined step based on the plaintext and the estimated parameter A;

an encryption control part for using and allowing an encryption apparatus to calculate ciphertext based on the plaintext accepted by the estimated stirred text calculating part;

a key verification part for formulating an encryption equation with higher order differences based on the predetermined-step estimated stirred text calculated by the estimated stirred text calculating part and the ciphertext calculated under the control of the encryption

control part, processing it by an algebraic technique to try to calculate a last-step extended key estimated as an extended key at a last step, verifying the parameter A_z to be right by detecting that the last-step estimated extended key can be calculated, calculating the last-step estimated extended key with a predetermined probability, and outputting a calculation impossible signal when detecting that calculation is impossible; and

a decryption control part for accepting the calculation impossible signal, and controlling the estimated stirred text calculating part, the encryption control part, and the key verification part to allow the last-step estimated extended key to be calculated.

7. (Currently Amended) A cipher strength evaluation apparatus for evaluating strength on ciphertext outputted by a Feistel encryption apparatus having a plurality of steps of accepting unstirred text, stirring with an extended key, and calculating stirred text for encrypting plaintext step by step, the cipher strength evaluation apparatus comprising:

an estimated stirred text calculating part for accepting the plaintext satisfying a predetermined condition, calculating an estimated parameter A_z estimated as a parameter A_z determined from a first-step extended key being an extended key at a first step, and calculating predetermined-step estimated stirred text satisfying a predetermined condition and estimated as stirred text at a predetermined step based on the plaintext and the estimated parameter A;

an encryption control part for using and allowing an encryption apparatus to calculate ciphertext based on the plaintext accepted by the estimated stirred text calculating part;

a second predetermined-step estimated stirred text calculating part for accepting the ciphertext calculated under the control of the encryption control part, calculating a last-step estimated extended key estimated as an extended key at a last step, and calculating second

predetermined-step estimated stirred text estimated as stirred text at a second predetermined step based on the ciphertext and the last-step estimated extended key;

a key verification part for formulating an encryption equation with higher order differences based on the predetermined-step estimated stirred text stirred text calculated by the estimated stirred text calculating part and the second predetermined-step estimated stirred text calculated by the second predetermined-step estimated stirred text calculating part, processing it by an algebraic technique to try to calculate a second predetermined-step extended key estimated as an extended key at the second predetermined step, verifying the parameter A and the last-step estimated extended key to be right by detecting that the second predetermined-step extended key can be calculated, and outputting a calculation impossible signal when detecting that calculation is impossible; and

a decryption control part for accepting the calculation impossible signal, and controlling the estimated stirred text calculating part, the encryption control part, the second predetermined-step estimated stirred text calculating part, and the key verification part to allow the second predetermined-step estimated extended key to be calculated.

8. (Currently Amended) A cipher strength evaluation apparatus for evaluating strength on ciphertext outputted by a Feistel encryption apparatus having a plurality of steps of accepting unstirred text, stirring with an extended key, and calculating stirred text for encrypting plaintext step by step, the cipher strength evaluation apparatus comprising:

an estimated stirred text calculating part for accepting the plaintext satisfying a predetermined condition, calculating an estimated parameter A_s estimated as a parameter A_s determined from a first-step extended key being an extended key at a first step by exhaustive

search, and calculating first-step estimated stirred text satisfying a predetermined condition and estimated as stirred text at a first step based on the plaintext and the estimated parameter A;

an encryption control part for using and allowing an encryption apparatus to calculate ciphertext based on the plaintext accepted by the estimated stirred text calculating part;

a key verification part for formulating an encryption equation with higher order differences based on the first-step estimated stirred text calculated by the estimated stirred text calculating part and the ciphertext calculated under the control of the encryption control part, processing it by an algebraic technique to try to calculate a last-step estimated extended key estimated as an extended key at a last step, verifying the parameter A_s to be right by detecting that the last-step estimated extended key can be calculated, calculating the last-step estimated extended key with a predetermined probability, and outputting a calculation impossible signal when detecting that calculation is impossible; and

a decryption control part for accepting the calculation impossible signal, and controlling the estimated stirred text calculating part, the encryption control part, and the key verification part to allow the last-step estimated extended key to be calculated.

9. (Currently Amended) A cipher strength evaluation apparatus for evaluating strength on ciphertext outputted by a Feistel encryption apparatus having a plurality of steps of accepting unstirred text, stirring with an extended key, and calculating stirred text for encrypting plaintext step by step, the cipher strength evaluation apparatus comprising:

an estimated stirred text calculating part for accepting the plaintext satisfying a predetermined condition, calculating an estimated parameter A_s estimated as a parameter A_s determined from a first-step extended key being an extended key at a first step by exhaustive

search, and calculating first-step estimated stirred text satisfying a predetermined condition and estimated as stirred text at a first step based on the plaintext and the estimated parameter A;

an encryption control part for using and allowing an encryption apparatus to calculate ciphertext based on the plaintext accepted by the estimated stirred text calculating part;

a predetermined-step estimated stirred text calculating part for accepting the ciphertext calculated under the control of the encryption control part, calculating a last-step estimated extended key estimated as an extended key at a last step, and calculating predetermined-step estimated stirred text estimated as stirred text at a predetermined step based on the ciphertext and the last-step estimated extended key;

a key verification part for formulating an encryption equation with higher order differences based on the first-step estimated stirred text calculated by the estimated stirred text calculating part and the predetermined-step estimated stirred text calculated by the predetermined-step estimated stirred text calculating part, processing it by an algebraic technique to try to calculate a predetermined-step estimated extended key estimated as an extended key at the predetermined step, verifying the parameter A_x and the last-step estimated extended key to be right by detecting that the predetermined-step estimated extended key can be calculated, and outputting a calculation impossible signal when detecting that calculation is impossible; and

a decryption control part for accepting the calculation impossible signal, and controlling the estimated stirred text calculating part, the encryption control part, the predetermined-step estimated stirred text calculating part, and the key verification part to allow the predetermined-step estimated extended key to be calculated.

10. (Currently Amended) A cipher strength evaluation apparatus for evaluating strength on ciphertext outputted by a Feistel encryption apparatus having a plurality of steps of accepting unstirred text, stirring with an extended key, and calculating stirred text for encrypting plaintext step by step, the cipher strength evaluation apparatus comprising:

an estimated stirred text calculating part for accepting the plaintext satisfying a predetermined condition, calculating an estimated parameter A_s estimated as a parameter A_s determined from a first-step extended key being an extended key at a first step by exhaustive search, and calculating first-step estimated stirred text satisfying a predetermined condition and estimated as stirred text at a first step based on the plaintext and the estimated parameter A;

an encryption control part for using and allowing an encryption apparatus to calculate ciphertext based on the plaintext accepted by the estimated stirred text calculating part;

a last-but-one-step estimated stirred text calculating part for accepting the ciphertext calculated under the control of the encryption control part, calculating a last-step estimated extended key estimated as an extended key at a last step by exhaustive search, and calculating last-but-one-step estimated stirred text estimated as stirred text at a last-but-one step based on the ciphertext and the last-step estimated extended key;

a key verification part for formulating an encryption equation with higher order differences based on the first-step estimated stirred text accepted by the estimated stirred text calculating part and the last-but-one-step estimated stirred text calculated by the last-but-one-step estimated stirred text calculating part, processing it by an algebraic technique to try to calculate a last-but-one-step extended key estimated as an extended key at the last-but-one step, verifying the parameter A and the last-step estimated extended key to be right by detecting that calculation

is possible, and outputting a calculation impossible signal when detecting that calculation is impossible; and

a decryption control part for accepting the calculation impossible signal, and controlling the estimated stirred text calculating part, the encryption control part, the last-but-one-step estimated stirred text calculation part and the key verification part to allow the last-but-one-step estimated extended key to be calculated.

11. (New) The cipher strength evaluating apparatus of Claim 1 wherein the parameter A allows an extended key to be calculated by simple logic operation with a known value.

12. (New) The cipher strength evaluating apparatus of Claim 1 wherein the parameter A is an equivalent key that an extended key is XOR-ed with a constant.